

In the Claims

1. (Currently Amended) A computerized method comprising:
obtaining data from a device for use as an input to a first cryptographic process;
creating an output of the first cryptographic process wherein the output comprises
a plurality of authorization levels; and
writing the output from the first cryptographic process to a storage location after
the device is received by a particular user in a plurality of users that are
authorized to use the device, wherein each authorization level is associated
with one of the plurality of users.
2. (Original) The method as set forth in claim 1, wherein the first cryptographic process is
based on a time stamp.
3. (Currently Amended) The method as set forth in claim 1, wherein the data is obtained
from the particular user.
4. (Original) The method as set forth in claim 3, wherein the data is entered with at least
one of a biometric device, a keypad, and a microphone.
5. (Original) The method as set forth in claim 1, further comprising creating an output of
a second cryptographic process, wherein the data is used as an input to the second
cryptographic process.
6. (Original) The method as set forth in claim 5, wherein the second cryptographic
process is based on a time stamp.
7. (Previously Presented) The method as set forth in claim 5, wherein the second
cryptographic process is performed by at least one of a device, a point of sale terminal, a
transaction privacy clearing house, a vendor, and a financial processing system.

8. (Original) The method as set forth in claim 5, further comprising comparing at least one of the output of the first cryptographic process and the input to the first cryptographic process with at least one of the output of the second cryptographic process and the input to the second cryptographic process.

9. (Original) The method as set forth in claim 8, further comprising allowing a transaction based on the comparing.

10. (Original) The method as set forth in claim 8, further comprising preventing the transaction based on the comparing.

11. (Currently Amended) The method as set forth in claim 8, wherein the comparing occurs without providing an identity of the particular user.

12. (Previously Presented) The method as set forth in claim 1, wherein one of the plurality of authorization levels comprises a limit on transactions to be authorized, the limit being at least one of:

- limiting an amount of money to be spent in a given time period;
- barring certain users from making certain types of transactions; and
- barring certain types of transactions.

13. (Original) The method as set forth in claim 1, wherein the storage location is selected from the group consisting of a magnetic stripe, a magnetic stripe emulator, a bar code emulator, and a personal transaction card.

14. (Currently Amended) A computer readable medium containing executable computer program instructions, which when executed by a data processing system, cause the data processing system to perform a method comprising:

- obtaining data from a device for use as an input to a first cryptographic process;
- creating an output of the first cryptographic process wherein the output comprises

a plurality of authorization levels; and
writing the output from the first cryptographic process to a storage location after
the device is received by a particular user in a plurality of users that are
authorized to use the device, wherein each authorization level is associated
with one of the plurality of users.

15. (Original) The computer readable medium as set forth in claim 14, wherein the first cryptographic process is based on a time stamp.

16. (Currently Amended) The computer readable medium as set forth in claim 14, wherein the data is obtained from the particular user.

17. (Original) The computer readable medium as set forth in claim 16, wherein the data is entered with at least one of a biometric device, a keypad, and a microphone.

18. (Original) The computer readable medium as set forth in claim 14, the method further comprises creating an output of a second cryptographic process, wherein the data is used as an input to the second cryptographic process.

19. (Original) The computer readable medium as set forth in claim 18, wherein the second cryptographic process is based on a time stamp.

20. (Previously Presented) The computer readable medium as set forth in claim 18, wherein the second cryptographic process is performed by at least one of a device, a point of sale terminal, transaction privacy clearing house, a vendor, and a financial processing system.

21. (Original) The computer readable medium as set forth in claim 18, the method further comprises comparing at least one of the output of the first cryptographic process and the input to the first cryptographic process and at least one of the output of the second cryptographic process and the input to the second cryptographic process.

22. (Original) The computer readable medium as set forth in claim 21, the method further comprises allowing a transaction based on the comparing.

23. (Original) The computer readable medium as set forth in claim 21, the method further comprises preventing a transaction based on the comparing

24. (Currently Amended) The computer readable medium as set forth in claim 21, wherein the comparing occurs without providing an identity of the particular user.

25. (Previously Presented) The computer readable medium as set forth in claim 14, wherein one of the authorization levels comprises a limit on transactions to be authorized, the limit being at least one of:

- limiting an amount of money to be spent in a given time period;
- barring certain users from making certain types of transactions; and
- barring certain types of transactions.

26. (Original) The computer readable medium as set forth in claim 14, wherein the storage location is selected from the group consisting of a magnetic stripe, a magnetic stripe emulator, a bar code emulator, and a personal transaction card.

27. (Currently Amended) An apparatus comprising:

security logic used to perform a first cryptographic process wherein an input to the first cryptographic process results in an output of the first cryptographic process wherein the output comprises a plurality of authorization levels, and wherein each one of the plurality of authorization levels is associated with a different one of a plurality of users that are authorized to use an electronic device coupled to the security logic; and wherein the electronic a device is communicatively coupled with the security logic and configured to write the output of the first cryptographic process to a storage location after the electronic device is received by a particular one

of the plurality of users.

28. (Original) The apparatus as set forth in claim 27, wherein the storage location is a magnetic stripe emulator.

29. (Original) The apparatus as set forth in claim 27, wherein the storage location is a bar code emulator.

30. (Original) The apparatus as set forth in claim 27, wherein the storage location is associated with a personal transaction card.

31. (Original) The apparatus as set forth in claim 30, wherein the storage location is a magnetic stripe.

32. (Original) The apparatus as set forth in claim 27, wherein the first cryptographic process is based on a time stamp.

33. (Original) The apparatus as set forth in claim 27, further comprising a user interface communicatively coupled with the security logic, wherein the input to the first cryptographic process comprises data entered from the user interface.

34. (Original) The apparatus as set forth in claim 33, wherein the user interface is at least one of a keypad, a biometric unit, and a microphone.

35. (Previously Presented) The apparatus as set forth in claim 27, wherein the security logic comprises logic that confirms an identification, the identification selected from the group consisting of a personal identification numbercode, voice identification, DNA identification, and biometric data.

36. (Previously Presented) The apparatus as set forth in claim 27, wherein one of the plurality of authorization levels comprises a limit on transactions to be authorized, the limit being at least one of:

- limiting an amount of money to be spent in a given time period;
- barring certain users from making certain types of transactions; and
- barring certain types of transactions.

37. (Currently Amended) An apparatus comprising:

a transaction terminal configured to communicate with a device, wherein an output of a first cryptographic process is read from the device by the transaction terminal and the first cryptographic process and a second cryptographic process are used to validate a transaction, the output comprising a plurality of authorization levels, wherein a plurality of users are authorized to use the device, and wherein each authorization level is associated with one of the plurality of users.

38. (Previously Presented) The apparatus as set forth in claim 37, wherein the second cryptographic process to be performed by at least one of a transaction terminal, a financial processing system, a transaction privacy clearing house, the device, and a vendor.

39. (Previously Presented) The apparatus as set forth in claim 37, wherein the transaction terminal is selected from the group consisting of a point of sale terminal, home computer system, bank automatic teller machine terminal, digital television, internet appliance, and personal point of sale terminal.

40. (Original) The apparatus as set forth in claim 37, wherein the second cryptographic process is based on a time stamp.

41. (Original) The apparatus as set forth in claim 37, wherein a comparison of at least one of the output of the first cryptographic process and the input to the first cryptographic process with at least one of an output of the second cryptographic process and an input to

the second cryptographic process allows a transaction if a result of the comparison is within a predetermined range.

42. (Original) The apparatus as set forth in claim 41, wherein the comparison occurs at the transaction terminal.

43. (Currently Amended) The apparatus as set forth in claim 41, wherein the comparison occurs without providing an identity of the plurality of users.

44. (Original) The apparatus as set forth in claim 37, wherein a comparison of at least one of the output of the first cryptographic process and the input to the first cryptographic process with at least one of an output of the second cryptographic process and an input to the second cryptographic process prevents a transaction.

45. (Original) The apparatus as set forth in claim 44, wherein the comparison occurs at the transaction terminal.

46. (Original) The apparatus as set forth in claim 44, wherein the comparison occurs without providing an identity of the user.

47. (Previously Presented) The apparatus as set forth in claim 37, wherein the device comprises: a personal transaction card.

48-56. (Cancelled)

57. (Previously Presented) The apparatus as set forth in claim 37, wherein one of the plurality of authorization levels comprises a limit on transactions to be authorized, the limit being at least one of:

- limiting an amount of money to be spent in a given time period;
- barring certain users from making certain types of transactions; and
- barring certain types of transactions.